MTH 236, Spring 2024 - Homework 13

Due on April 26th at 11:59pm on gradescope

1. True or false? Provide brief justifications for your answers.

   (a) $a^{p-1} \equiv 1 \pmod{p}$ for all integers a and primes p.

   (b) $\varphi(n)$ can never equal n for a positive integer $n \geq 2$ (where $\varphi(n)$ represents the Euler φ function).

   (c) There exists a ring homomorphism $\phi : \mathbb{Q} \longrightarrow \mathbb{Q}$ whose kernel is $\mathbb{Z}$.

   (d) Every factor ring of a commutative ring is a commutative ring

   (e) An ideal of a ring with unity is the entire ring if and only if it contains the multiplicative identity.

2. Find $q(x)$ and $r(x)$ such that $f(x) = q(x)g(x) + r(x)$ with $r(x) = 0$ or $\deg(r) < \deg(g)$

   (a) $f(x) = x^6 + 3x^5 + x + 1$ and $g(x) = x^2 + 2x - 1$ in $\mathbb{Z}_7[x]$.

   (b) $f(x) = x^6 + 3x^5 + x + 1$ and $g(x) = 3x^2 + 2x - 1$ in $\mathbb{Z}_7[x]$.

   (c) $f(x) = x^4 + 5x^3 - 3x^2$ and $g(x) = 5x^2 - x + 2$ in $\mathbb{Z}_{11}[x]$.

3. (a) Show that $x^2 + x + 1$ is irreducible in $\mathbb{Z}_5[x]$ and in $\mathbb{Z}_{29}[x]$.

   (b) Show that $x^3 - a$ is irreducible in $\mathbb{Z}_7[x]$ unless $a = 0$ or ± 1.

   (c) Determine how $x^5 + 1$ factors into irreducible polynomials in $\mathbb{Z}_2[x]$.

4. Prove that every (ring) homomorphism from a field to a ring that is not one-to-one, must be trivial i.e., maps everything in the field to 0.

5. Let R and R' be rings, $\phi : R \mapsto R'$ a ring homomorphism and N an ideal of R.

   (a) Prove that $\phi[N]$ is an ideal of $\phi[R]$.

   (b) Give an example to show that $\phi[N]$ need not be an ideal of R'.

   (c) Let N' be an ideal of $\phi[R]$. Prove that $\phi^{-1}[N']$ is an ideal of R.

6. Let R be a ring and let I, J be two ideals in R.

(a) Prove that $I \cap J$ is an ideal of R. Show it is the largest ideal contained in both I and J, in the sense that every ideal contained in both I and J is a subset of $I \cap J$.

(b) Define $I + J$ by

$$I + J = \{x + y \,|\, x \in I, y \in J\}.$$

Prove that $I + J$ is an ideal. Show it is the smallest ideal containing both I and J, in the sense that every ideal containing both I and J must also contain $I + J$.

7. Let R be a commutative ring. An element $a \in R$ is said to be *nilpotent* if $a^n = 0$ for some $n \in \mathbb{Z}^+$.

(a) Prove that the set of all nilpotent elements

$$N = \{a \in R \,|\, a^n = 0 \text{ for some } n \in \mathbb{Z}^+\}$$

is an ideal of R. [Hint: If $a^n = 0$ and $b^m = 0$, consider $(a + b)^{(m+n)}$.]

(b) Now prove that the only nilpotent element in the factor ring R/N is the zero coset $N = 0 + N$.

8. For each of the following, give an example if possible. If not possible, briefly explain why not.

(a) A commutative ring that does not have a unity element.

(b) A commutative ring with unity that is not an integral domain.

(c) A non-commutative ring that has a unity element.

(d) A non-commutative ring that does not have a unity element.

(e) A field that is not an integral domain.

(f) An integral domain that is not a field.

(g) A finite integral domain that is not a field.